自适应分块的医学图像混沌加解密算法 *

拜亚萌 [1]，张燕玲 [1]，邓小鸿 [2†]

(1. 焦作大学 信息工程学院, 河南 焦作 454000; 2. 江西理工大学 应用科学学院, 江西 赣州 341000)

摘　要：针对现有基于混沌的医学图像加密算法未考虑图像纹理特征的不足，提出了一种自适应分块的医学图像混沌加解密算法。算法首先利用 2D Sine Logistic 混沌系统生成两个具有良好混沌特性的安全序列；然后将图像分成固定尺寸的图像块，并计算图像块的最大像素差和方差，根据设定的阈值将图像块划分成纹理平滑块和纹理复杂块；最后利用混沌序列 1 对平滑块进行密文反馈加密，利用混沌序列 2 对复杂块进行明文反馈加密，得到加密后的图像。算法有效考虑了图像块的纹理特性，优化了混沌加密算法，提高了医学图像的加解密效率。实验仿真结果表明，提出的算法具有高的安全性和加解密效率，相比现有方法加解密速度提高 1 倍左右。算法适用于大数据量的医学图像实时加解密。

关键词：医学图像；数据加密；混沌映射；纹理复杂度；自适应分块

中图分类号：TP309.7　　doi: 10.19734/j.issn.1001-3695.2018.10.0830

Digital medical image encryption and decryption algorithm based on chaotic mapping and adaptive partitioning

Bai Yameng[1], Zhang Yanling[1], Deng Xiaohong[2†]

(1. *College of Information Engineering*, *Jiaozuo University*, *Jiaozuo* Henan 454000, *China*; 2. *College of Applied Science*, *Jiangxi University of Science & Technology*, *Ganzhou* Jiangxi 341000, *China*)

Abstract: In order to solve the weakness of existing medial image encryption algorithm based on chaotic system in considering the image's texture feature, this paper proposed a medical image encryption and decryption method based on chaotic mapping and adaptive partitioning. Firstly, it used the 2D Sine Logistic chaotic system to generate two secure sequences with good chaotic characteristics. Then, it divided the original medical image into fixed size image blocks, and calculated their maximum pixel difference and variance. According to the given threshold, it divided these image blocks into texture smooth blocks and texture complex blocks. Finally, it used the first chaotic sequence with ciphertext feedback mechanism to encrypt the smooth blocks, and encrypt the complex blocks by using the second chaotic sequence with plaintext feedback mechanism. Therefore, it obtained the encrypted image. Because the presented algorithm efficiently considers the texture characteristics of image blocks and optimizes the algorithm of chaotic encryption, it improves the encryption and decryption efficiency of medical images. Experimental simulation results show that the presented algorithm has high security and encryption efficiency. Compared with the existent method, it reduces the encryption and decryption time by about 0.5 times. The presented algorithm is suitable for real-time medical images encryption and decryption with big data size.

Key words: medical image; data encryption; chaotic mapping; texture complexity; adaptive partitioning.

0　引言

混沌系统由于具有大的密钥空间、高的初值敏感性、非周期性和伪随机性等优良特性，已经被广泛应用于密码学领域，并形成了现代密码学的一个新方向——混沌密码学[1,2]。利用混沌系统产生的序列作为流密码，对载体内容进行加密具有操作简单效率高的特点，在对大数据量的数字图像加密时具有优势[3~5]。医学图像相比自然图像，含有病人的重要隐私信息，并对医学诊断起着至关重要的作用，研究医学图像混沌加密算法在移动医疗和在线医疗领域具有重要意义。

相比自然图像，医学图像具有像素分布不均匀、图像轮廓分界明显（存在较明显的前景和背景区域）、图像分辨率高和数据量大等特点，造成了医学混沌加密算法需要更高安全性和效率。目前，具有代表性的研究成果集中在两个方面：一是加密算法安全性提升，研究者们发现单一或者低维的混沌系统存在着安全隐患，提出结合多个混沌系统或者设计超混沌系统等策略来保证安全。如 Kanso 等人[6]提出引入一个随机矩阵作为混沌加密过程中的置乱元素,增强了算法抗攻击的能力。Zhang 等人[7]提出设计新的超混沌系统并引入 DNA 序列计算方法来进行医学图像加密,DNA 序列本身具有高的随机性，算法的安全性得到极大提升。Wu 等人[8]综合应用 Chen 混沌、3D cat 映射和 logistic 混沌系统来实施医学图像加密。二是在加密算法效率方面提升，文献[9]重点改进了基于混沌序列加密算法中的像素置乱和扩散机制,提出了快速像素混淆方法，大大提高了加密速度。文献[10]提出将医学图像进行感兴趣区域和非感兴趣区域的划分，然后对含有重要诊断信息的感兴趣区域进行混沌加密，算法仅对图像的部分像素加密，效率更高，但由于医学图像中感兴趣区域的

收稿日期:2018-10-08;**修回日期:**2018-12-28　**基金项目:**国家自然科学基金资助项目(61762046);江西省自然科学基金资助项目(20161BAB212048)
作者简介:拜亚萌（1980-），男，讲师，硕士，主要研究方向为网络信息安全；张燕玲（1977-），女，讲师，硕士，主要研究方向为信息安全；邓小鸿（1982-），男（通信作者），副教授，博士，主要研究方向为网络信息安全（deng_xh@jxust.edu.cn）.

不规则性，区域的分割和几何表示具有高复杂性。文献[11，12]分别提出了基于频域的医学图像混沌加密方法，前者先将医学图像进行离散余弦变换，仅选取变换后的部分系数进行加密，但由于余弦变换存在着浮点数计算，算法的可逆性实施难度大；为了解决这一问题,文献[12]提出基于整数小波变换的医学图像混沌加密,选择三级小波分解的低频系数进行加密,算法较好地实施了可逆性,仅对低频系数加密提升了算法效率,但加密图像存在着较明显的轮廓现象,安全性不足。

综上所述，现有的医学图像混沌加密方法很难在算法的安全性和高效率之间得到较好的折中，原因在于算法绝大部分都没有考虑医学图像自身的纹理特征，针对不同的医学图像往往加密密钥都是一样的，难以实现"一次一密"，算法的安全性存在较大隐患，另外，超混沌系统和多混沌系统的引入会增大算法的复杂性。针对上述问题，本文提出了一种自适应分块的医学图像混沌加解密算法，将医学图像进行分块，并将块类型标志作为加密密钥的一部分，充分考虑到不同图像的自身纹理特征，并采用 2D Sine Logistic 混沌系统产生的密钥对不同纹理的图像块进行反馈加密，加密过程简单高效，保证了算法的时间效率。

1 相关知识

1.1 2D Sine Logistic 混沌系统

2D Sine Logistic 混沌系统由两个简单的一维混沌 Logistic 和 sine 组合而成，其数学表达式如式(1)(2)所示。

$$x_{i+1} = \alpha x_i(1-x_i) \tag{1}$$

$$x_{i+1} = u\sin(\pi x_i) \tag{2}$$

其中：α 和 u 为混沌控制参数，其值域分别为 $\alpha \in [0,4]$，$u \in [0,1]$。Logistic 和 sine 混沌系统结构简单，属于典型的一维混沌系统，已有研究者证明其存在安全隐患[13]。Hua 等人[14]提出了 2D Sine Logistic 混沌映射，并且证明了其在安全性和实现效率上相比其他高维混沌系统具有优势。2D Sine Logistic 混沌映射可表示为

$$\begin{cases} x_{i+1} = \alpha(\sin(\pi y_i) + \beta)x_i(1-x_i) \\ y_{i+1} = \alpha(\sin(\pi x_{i+1}) + \beta)y_i(1-y_i) \end{cases} \tag{3}$$

其中：$x_i, y_i \in [0,1]$，$\alpha \in [0,1]$，$\beta \in [0,3]$，当 $\alpha \in [0.905,1]$ 并且 β 接近 3 时，2D Sine Logistic 混沌映射具有超混沌行为。

1.2 图像的四叉树分解

图像的四叉树分解最早用于图像的分割，通过计算图像块中最大像素差是否满足指定的条件来确定一个图像块是否需要进行下一步的划分[15]。其判定条件如式(4)所示。

$$p_{max} - p_{min} > (2^d - 1)\times\gamma \tag{4}$$

其中：p_{max} 和 p_{min} 分别表示图像块中像素的最大值和最小值,d 为图像像素的位深度(如 256 色的图像 d=8),γ 为阈值,用来控制图像分解的块数。经过图像的四叉树分解后每个图像块内的像素具有高同质性,单个图像块属于图像的纹理平滑区域。

2 本文方法

2.1 图像纹理块划分

本文首先将原始医学图像进行固定尺寸（$size \times size$）的划分，然后获取图像块中最大和最小像素值，如果满足式(4)则得到图像块的类型 1，表示为

$$type_1 = \begin{cases} 1 & if\ \ p_{max} - p_{min} > (2^d - 1)\times\gamma \\ 0 & else \end{cases} \tag{5}$$

其次，根据如式(6)所示的方差计算方法，计算图像块的方差，根据式(7)得到图像块的类型 2，当图像块的类型 1 和 2 满足式(8)时，将图像块区分为纹理平滑块和纹理复杂块。

$$S = \frac{1}{n-1}\sum_{i=1}^{n}(X_i - \overline{X})^2 \tag{6}$$

$$type_2 = \begin{cases} 1 & if\ S > T \\ 0 & else \end{cases} \tag{7}$$

$$type = \begin{cases} 0 & if\ (type_1 == 0\ \&\&\ type_2 == 0) \\ 1 & else \end{cases} \tag{8}$$

式(6)中，S 为图像块方差，n 为图像块中像素个数，X_i 为单个像素值，$\overline{X}$ 为图像块像素均值；式(7)中，T 为方差阈值；式(8)中，当 $type$ 为 0 时代表当前图像块为纹理平滑块，为 1 时为纹理复杂块。

2.2 明密文反馈加解密机制

医学图像中，图像纹理平滑区域往往集中在图像的背景区域，其像素值集中在 0 附近，图像的明文反馈并不能起到应有的效果，本文采用如式(9)所示的密文反馈加密机制。相反，图像的纹理复杂区域集中在图像的前景区域，其像素值本身变化较明显，采用如式(10)所示的明文反馈机制。加密采用简单的异或操作，具有高效率和良好的可逆性。

$$\begin{cases} E_block(i) = block(i) \oplus seq_1(i) & if\ (i == 1) \\ E_block(i) = block(i) \oplus seq_1(i) \oplus E_block(i-1) & else \end{cases} \tag{9}$$

$$\begin{cases} E_block(i) = block(i) \oplus seq_2(i) & if\ (i == 1) \\ E_block(i) = block(i) \oplus seq_2(i) \oplus block(i-1) & else \end{cases} \tag{10}$$

其中：$block(i)$ 和 $E_block(i)$ 分别表示图像块中的原像素值和加密像素值，seq_1 和 seq_2 分别为采用 2D Sine Logistic 混沌系统产生的两个混沌序列，由于序列的值在[0,1]，需要采用式(11)所示方法进行调整(8bit 深度医学图像像素在 0~255)。

$$seq(i) = \mathrm{mod}(round(seq(i)\times 10^6), 256) \tag{11}$$

纹理平滑块的解密机制如式(12)所示，纹理复杂块的解密机制如(13)所示。

$$\begin{cases} R_block(i) = E_block(i) \oplus seq_1(i) & if\ (i == 1) \\ R_block(i) = E_block(i) \oplus seq_1(i) \oplus E_block(i-1) & else \end{cases} \tag{12}$$

$$\begin{cases} R_block(i) = E_block(i) \oplus seq_2(i) & if\ (i == 1) \\ R_block(i) = E_block(i) \oplus seq_2(i) \oplus R_block(i-1) & else \end{cases} \tag{13}$$

其中，R_block 为解密后的图像块。

2.3 算法模型

算法大致执行流程如图 1 所示。首先，原始医学图像进行固定尺寸 8×8 的分块，对于每个图像块利用式(5)~(8)进行纹理复杂度划分；其次利用 2D Sine Logistic 混沌系统生成与医学图像尺寸等长的二个混沌序列；然后，对平滑块用式(9)进行加密，对复杂块用式(10)进行加密。最后，将加密后的图像块组合得到最后的加密医学图像。解密时，只需将原始医学图像换成加密后的医学图像，对于平滑块和复杂度分别用式(12)(13)即可实施解密。

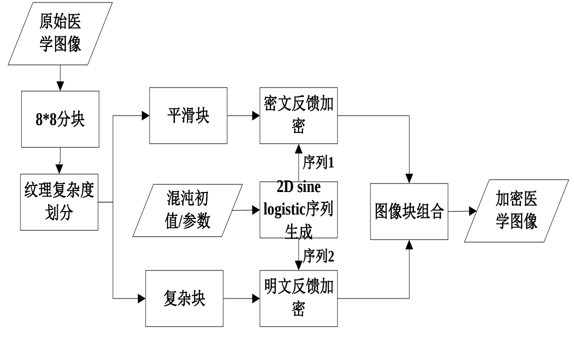


图 1 算法执行流程

Fig. 1 Execution process of the proposed algorithm

2.4 加解密算法

自适应分块医学图像混沌加密算法如算法 1 所示。

算法 1 自适应分块的医学图像混沌加密算法

Input: *I*（原始医学图像）；*γ*（四叉树分解阈值）；2D Sine Logistic 混沌系统初值、控制参数；方差阈值 T；分块尺寸 size。

Output: *EI*(加密医学图像)；*block_type*(原医学图像的块类型标志)。

```
read(I) ; //  读取原始医学图像
[M,N]=size(I) ; //  获取图像维数
set the initial value seq(1)/seq(2) and control parameter a、b;
[seq1,seq2]=D2_SLMM(a,b, seq(1),seq(2),M*N);//生成混沌序列
block=zeros(size,size);//初始化图像块数组
for p=1:M/size
    for q=1:N/size
    x=(p-1)*size+1;y=(q-1)*size+1;//计算图像块左上角坐标
    block=I(x:x+size-1,y:y+size-1);//获取单个图像块数据
     use formula (5)~(8) to judge this block's type;
     if  当前块为平滑块
         block_type(p,q)=0;//记录当前块类型标志
         use formula (9) to encrypt this block;
     else
         block_type(p,q)=1;//记录当前块类型标志
         use formula (10) to encrypt this block;
     end if
     EI(x:x+size-1,y:y+size-1) =block;//得到加密图像块
     end for
end for
return EI, block_type
```

自适应分块的医学图像混沌解算法如算法 2 所示：

算法 2 自适应分块的医学图像混沌解密算法

Input: *EI*（加密医学图像）；*γ*（四叉树分解阈值）；2D Sine Logistic 混沌系统初值、控制参数；方差阈值 T；分块尺寸 size；*block_type*。

Output: *RI*（解密医学图像）。

```
read(EI) ; //  读取加密医学图像
[M,N]=size(EI) ; //  获取图像维数
set the initial value seq(1)/seq(2) and control parameter a、b;
[seq1,seq2]=D2_SLMM(a,b, seq(1),seq(2),M*N);//生成混沌序列
block=zeros(size,size);//初始化图像块数组
for p=1:M/size
    for q=1:N/size
    x=(p-1)*size+1;y=(q-1)*size+1;//计算图像块左上角坐标
    block=I(x:x+size-1,y:y+size-1);//获取单个图像块数据
     if block_type(p,q)==0//当前块为平滑块
         use formula (12) to decrypt this block;
     else
         use formula (13) to decrypt this block;
     end if
     RI(x:x+size-1,y:y+size-1) =block;//得到解密图像块
     end for
end for
return RI
```

2.5 方法创新点及可行性分析

方法的创新之处主要体现在两个部分：a）将图像划分成纹理复杂区域和纹理平滑区域，针对不同的区域提出自适应的加密算法，充分考虑到图像的自身纹理特征，实施"一次一密"；b）设计了基于 2D Sine Logistic 混沌序列的明密文反馈机制，解决单一加密机制带来的安全性不足问题。方法采用图像四叉树分解和方差计算方法来判断图像的纹理块，计算方法简单有效，另外基于异或的加解密策略执行速度快，保证了算法的执行效率。

3 实验结果与分析

3.1 实验环境与参数设置

实验中选取 4 幅不同纹理结构的医学图像 x-ray、us、ct、mri（均来自于中南大学湘雅医学院，512×512 尺寸，jpg 格式），为了测试算法在不同尺寸和格式图像中的加密效率，将 mri 图像分别缩小尺寸为 128×128 和 256×256，并以 bmp 格式进行存储。实验主机配置环境：Matlab7.0，CPU 为 Intel(R) Core™ i5-6500 3.20 GHz，内存 8 GB，64 位 Windows 7 旗舰版操作系统。实验中设定 2D Sine Logistic 混沌的初值 seq(1)=0.9380，seq(2)=0.7006，控制参数 a=1,b=3。四叉树分解阈值设为 0.04(图像块中最大像素差在 10 左右，人的肉眼如法察觉到 10 以内的灰度变化)，方差阈值 T 设为 5。4 幅医学图像及对应的加密效果如图 2 所示。

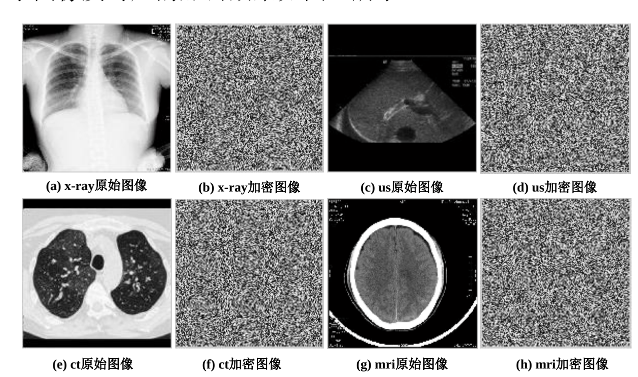


图 2 医学图像及其加密结果

Fig. 2 The medical images and its encryption results

3.2 算法安全性分析

3.2.1 密钥安全性

密钥安全性通常由密钥空间和密钥敏感性衡量。本文算法的加密密钥由以下部分组成：分块尺寸 size、四叉树分解阈值 *γ*、方差阈值 *T*、混沌系统的两个初值和两个控制参数组成，每个参数为 4 字节，则加密密钥空间为 2^{224}，采用穷举攻击方法在计算上是不可能的。解密密钥在加密密钥基础上增加了图像块类型标志，当分块尺寸为 8 时，一幅 512×512 尺寸的图像的块类型标志为4096 bit，解密密钥空间为 2^{4320}。为了测试密钥敏感性，将混沌序列初值 seq(1)修改为 0.9380004，seq(2)修改为 0.7006001，设默认密钥为 key，修改后密钥为 key1，其他参数不变。图 3 给出了密钥敏感性的测试结果，图 3(a)是 ct 图像采用 key 和 key1 加密后图像的差，图 3(b)是对图 2(f)中图像采用 key1 解密后的图像。从图 3 中可以看出，即使微小的密钥参数改变，也会带来加密图像的截然不同，并且也无法正确解密出原始图像。

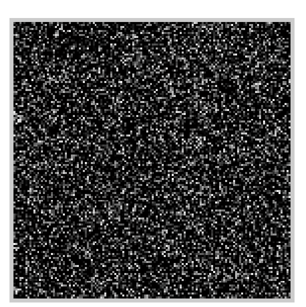
3.2.2 抗统计攻击分析

加密图像信息熵越接近与理想值 8，算法的抗统计攻击能力越强，表 1 给出了不同载体图像采用本文方法进行加密后加密图像的信息熵，并与文献[14]进行了对比。从表 1 中结果可以看出本文方法得到的加密图像信息熵达到 7.999 左右，并且与文献[14]结果几乎一致。

加密图像相邻像素之间的相关性也是衡量算法抗攻击性的重要指标，采用式(14)量化相邻像素之间的相关性。

$$corr=\frac{\sum_{i=1}^{num}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{(\sum_{i=1}^{num}(x_i-\bar{x})^2)(\sum_{i=1}^{num}(y_i-\bar{y})^2)}} \tag{14}$$

其中：x_i 和 y_i 分别表示第 i 组相邻的像素对，$\bar{x}$ 和 $\bar{y}$ 分别表示相邻像素的平均值，*num* 为相邻像素对数。*corr* 值越接近 1 代表相邻像素相关性越高，接近 0 代表相关性越低。表 2 给出 ct 图像分别取 50 组相邻像素对（水平、垂直和对角线方向）的相关性测试结果。从表 2 中可以看出，医学图像明文相邻像素具有高相似性，但通过本文算法加密后，密文中相邻像素相关系数值在 0.001 左右，接近理想值 0。


(a)加密图像差

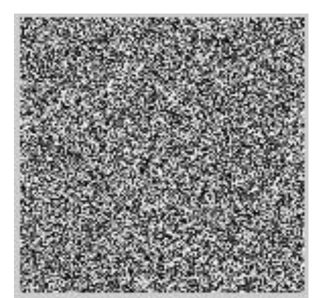

(b)解密图像

图 3　密钥敏感性结果

Fig. 3　Results of key sensitivity

表 1　加密图像信息熵

Table 1　Information entropy of the encrypted images

载体图像	文献[14]	本文方法
mri.bmp(128×128)	7.9882	7.9868
mri.bmp(256×256)	7.9972	7.9968
mri.jpg(512×512)	7.9992	7.9993
us.jpg(512×512)	7.9993	7.9993
xray.jpg(512×512)	7.9992	7.9992
ct.jpg(512×512)	7.9993	7.9993

表 2　像素相关性测试结果

Table 2　Testing results of pixel correlation

载体图像	水平方向	垂直方向	对角线方向
ct.jpg 明文	0.9876	0.9749	0.9802
ct.jpg 密文	0.0012	0.0019	0.0011

3.2.3 抗差分攻击分析

抗差分攻击能力通过密文对明文的敏感程度衡量，本文选取像素值平均改变强度(unified average changing intensity, UACI)来测试，其计算表达式如式(15)所示。

$$UACI = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|E_1(i,j) - E_2(i,j)|}{255} \times 100\% \qquad (15)$$

其中：M 和 *N* 为图像尺寸，$E_1(i,j)$ 和 $E_2(i,j)$ 分别为原始图像仅有一个像素点不同得到的加密图像。

根据文献[12]结论，*UACI* 的理想值为 33.4635%，图 4 给出了 CT 图像 *UACI* 值测试结果。测试中选用 50 组图像(每副载体图像随机修改 1 个不同位置的像素点，与原图组成一组)，对每组进行编号，分别计算每组的 *UACI* 值。从图 4 中可以看出，*UACI* 值在理想值上下波动，说明算法具有较强的抗差分攻击能力。

3.2.4 算法执行效率分析

本文算法的加解密时间和与文献[14，16]的对比结果如表 3 所示。表中结果均为测试 10 次之后的平均值，为了统一比较标准，将文献[14，16]方法在本文的实验环境中进行了仿真。从表 3 中可以看出，本文方法的加解密时间明显小于文献[14，16]方法，当图像尺寸达到 512×512 时，本文加解密时间约为文献[14]方法的一半。虽然两个方法都是对医学图像所有的像素进行了扩散加密，但文献[14]除了对像素进行扩散机密外，引入了两轮位置置乱，增加了加密算法的复杂度。文献[16]将原始医学图像首先采用 Logistic-sine 混沌映射加密，然后对加密后的图像进行 2*2 分块，并对每个块进行超混沌加密，方法虽然也提出了自适应性概念，但仅仅局限于将不同图像块的内容采用反馈机制加入到加密过程中，并且超混沌系统的引入增大了算法的复杂度，造成了加解密效率在三种方法中最低。而本文方面充分考虑图像块纹理特征，采用简单的明密文反馈加密提高了算法执行效率。

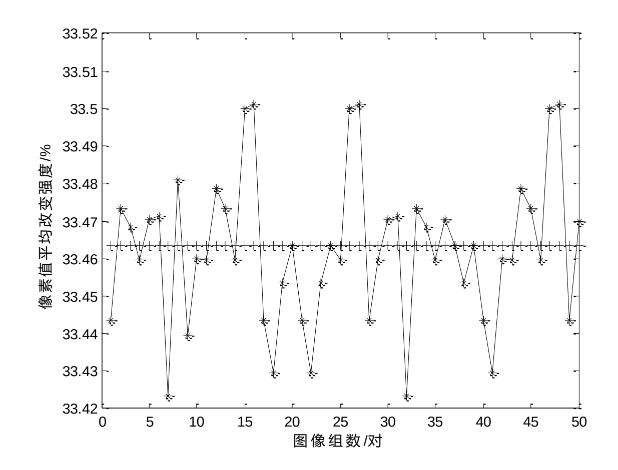


图 4　UACI 测试结果

Fig. 4　The testing results of UACI

表 3　本文算法加解密效率测试结果

Table 3　Encrypt efficiency testing results of the proposed algorithm

载体图像	文献[14]		文献[16]		本文方法	
	加密时间/s	解密时间/s	加密时间/s	解密时间/s	加密时间/s	解密时间/s
mri.bmp(128×128)	0.610	0.595	0.879	0.877	0.348	0.323
mri.bmp(256×256)	8.126	8.094	10.255	10.198	3.334	3.161
mri.jpg(512×512)	41.144	41.019	46.294	45.988	19.285	18.992
us.jpg(512×512)	40.977	40.678	47.046	46.875	19.264	18.969
xray.jpg(512×512)	41.354	41.017	46.374	46.226	19.167	18.981
ct.jpg(512×512)	41.023	40.988	47.054	46.882	19.209	18.997

4　结束语

算法利用像素最大像素差和方差计算方法对图像块进行简单有效的纹理分类，针对不同纹理的图像块采用不同的加密方法，算法充分考虑到了图像局部区域的纹理特征，密钥由明文图像组成，实现了“一次一密”的加解密，算法的安全性得到提升。简单高效的基于混沌序列的反馈加密机制确保了算法的时间效率。本文方法首次提出将医学图像按照纹理复杂度分块后实施加密，为医学图像的分区域加密提供了新的思路。但本文的方法有一定的局限性，图像块的纹理特征分类过于粗糙，下一步将考虑更为科学的图像纹理复杂度划分方法。

参考文献：

[1] 禹思敏，吕金虎，李澄清. 混沌密码及其在多媒体保密通信中应用的进展 [J]. 电子与信息学报, 2016, 38(3): 735-752. (Yu Simin, Lv Jinhu, Li Chengqin. Some progresses of chaotic cipher and its applications in multimedia secure communications [J]. Journal of Electronics & Information Technology, 2016, 38(3): 735-752.)

[2] Li Ming, Guo Yuzhu, Huang Jie, *et al.* Cryptanalysis of a chaotic image encryption scheme based on permutation-diffusion structure [J]. Signal Processing: Image Communication, 2018, 62(3): 164-172.

[3] 葛滨，鲁华祥，陈旭，等. 基于超混沌的快速图像加密算法 [J]. 系统工程与电子技术，2016, 38(3): 699-705. (Ge Bin, Liu Huaxiang, Chen Xu, *et al.* Fast image encryption algorithm based on hyper-chaos [J]. Systems Engineering and Electronics, 2016, 38(3): 699-705.)

[4] Silva-Garcia V M, Flores-Carapia R, Renteria-Marquez C, *et al.* Substitution box generation using Chaos: an image encryption application [J]. Applied Mathematics and Computation, 2018, 332(9): 123-135.

[5] 闫兵，柏森，刘博文，等. 基于交叉混沌映射的小波域图像加密算法 [J]. 计算机应用研究, 2018, 36(6): 1797-1799. (Yan Bing, Bai Sen, Liu Bowen, *et al.* Algorithm of image encryption in wavelet domain based on cross chaotic map [J]. Application Research of Computers, 2018, 36(6): 1797-1799.)

[6] Kanso A, Ghebleh M. An efficient and robust image encryption scheme for medical applications [J]. Communications in Nonlinear Science and Numerical Simulation, 2015, 24(1-3): 98-116.

[7] Zhang Limin, Sun Kehui, Liu Wenhao, *et al.* A novel color image encryption scheme using fractional-order hyperchaotic system and DNA sequence operations [J]. Chinese Physics, 2017, 26(10): 98-106.

[8] Wu Jiahui, Liao Xiaofeng, Yang Bo. Cryptanalysis and enhancements of image encryption based on three-dimensional bit matrix permutation [J]. Signal Processing, 2018, 142(1): 292-300.

[9] Hua Zhongyun, Yi Shuang, Zhou Yicong. Medical image encryption using high-speed scrambling and pixel adaptive diffusion [J]. Signal Processing, 2018, 144(3): 134-144.

[10] Pareek N K, Patidar V. Medical image protecting using genetic algorithm operations [J]. Soft Computing, 2016, 20(2): 763-772.

[11] Lima J B, Madeiro F, Sales F J R. Encryption of medical images based on the cosine number transform [J]. Signal Processing: Image Communication, 2015, 35(1): 1-8.

[12] 梁涤青，陈志刚，邓小鸿. 基于超混沌映射的医学图像小波域加密算法 [J]. 天津大学学报 :自然科学与工程技术版，2016, 49(12): 1255-1261. (Liang Diqing, Chen Zhigang, Deng Xiaohong. Encryption method of medical image based on wavelet transform and hyper-chaotic mapping [J]. Journal of Tianjin University:Science and Technology , 2016, 49(12): 1255-1261.)

[13] 陈志刚，梁涤青，邓小鸿，等. Logistic 混沌映射性能分析与改进 [J]. 电子与信息学报, 2016, 38(6): 1547-1551. (Chen Zhigang, Liang Diqing, Deng Xiaohong, *et al.* Performance analysis and improvement of logistic chaotic mapping [J]. Journal of Electronics & Information Technology, 2016, 38(6): 1547-1551.)

[14] Hua Zhongyun, Zhou Yicong, Pun C M, *et al.* 2D Sine Logistic modulation map for image encryption [J]. Information Sciences, 2015, 297(C): 80-94.

[15] Spann M, Wilson R. A quad-tree approach to image segmentation which combines statistical and spatial information [J]. Pattern Recognition, 1985, 18(3-4): 257-269.

[16] Chen Xiao, Hu Chunjie. Adaptive medical image encryption algorithm based on multiple chaotic mapping [J]. Saudi Journal of Biological Sciences, 2017, 24(8): 1821-1827.